January 27, 2005

Information Technology Management

Management of Information Technology Resources Within DoD
(D-2005-029)

Department of Defense
Office of the Inspector General

Quality *Integrity* *Accountability*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
27 JAN 2005	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Information Technology Management: Management of Information Technology Resources Within DoD	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Inspector General Department of Defense 400 Army Navy Drive Arlington, VA 22202-4704**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**27**	

Additional Copies

To obtain additional copies of this report, visit the Web site of the Inspector General of the Department of Defense at http://www.dodig.osd.mil/audit/reports or contact the Secondary Reports Distribution Unit, Audit Followup and Technical Support at (703) 604-8937 (DSN 664-8937) or fax (703) 604-8932.

Suggestions for Future Audits

To suggest ideas for or to request future audits, contact Audit Followup and Technical Support at (703) 604-8940 (DSN 664-8940) or fax (703) 604-8932. Ideas and requests can also be mailed to:

ODIG-AUD (ATTN: AFTS Audit Suggestions)
Inspector General of the Department of Defense
400 Army Navy Drive (Room 801)
Arlington, VA 22202-4704

Acronyms

BMMP	Business Management Modernization Program
DITPR	DoD Information Technology Portfolio Repository
EA	Enterprise Architecture
FISMA	Federal Information Technology Security Management Act
FMFIA	Federal Managers Financial Integrity Act
GAO	Government Accountability Office
GIG	Global Information Grid
IG DoD	Inspector General Department of Defense
IT	Information Technology
ITMA	Information Technology Management Application.
MID	Management Initiative Decision
OMB	Office of Management and Budget

INSPECTOR GENERAL
DEPARTMENT OF DEFENSE
400 ARMY NAVY DRIVE
ARLINGTON, VIRGINIA 22202-4704

January 27, 2005

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE
(COMPTROLLER)/CHIEF FINANCIAL OFFICER
ASSISTANT SECRETARY OF DEFENSE FOR NETWORKS
AND INFORMATION INTEGRATION/CHIEF
INFORMATION OFFICER

SUBJECT: Report on Management of Information Technology Resources Within DoD (Report No. D-2005-029)

We are providing this report for review and comment. The Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not respond to the draft report.

DoD Directive 7650.3 requires that all recommendations be resolved promptly. All recommendations remain unresolved. Therefore, we request that the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer provide comments on this final report by February 28, 2005.

If possible, please send management comments in electronic format (Adobe Acrobat file only) to Audam@dodig.osd.mil. Copies of the management comments must contain the actual signature of the authorizing official. We cannot accept the / Signed / symbol in place of the actual signature. If you arrange to send classified comments electronically, they must be sent over the SECRET Internet Protocol Router Network (SIPRNET).

We appreciate the courtesies extended to the staff. Questions should be directed to Ms. Kathryn M. Truex at (703) 604-8966 (DSN 664-8966) or Mr. Thomas S. Bartoszek at (703) 604-9049 (DSN 664-9049). See Appendix E for the report distribution. The team members are listed inside the back cover.

By direction of the Deputy Inspector General for Auditing:

Mary L. Ugone
Assistant Inspector General
for Acquisition and Technology Management

Office of the Inspector General of the Department of Defense

Report No. D-2005-029 **January 27, 2005**
(Project No. D2004AL-0139)

Management of Information Technology Resources Within DoD

Executive Summary

Who Should Read This Report and Why? Officials responsible for management of DoD information technology and officials responsible for the acquisition and management of information systems should read this report. The report discusses the need to establish an inventory of DoD information systems and build a consistent governance structure for information technology that will enhance management of DoD information resources and allow DoD to respond accurately to information requests from Congress and the Office of Management and Budget.

Background. The E-Government Act of 2002, Public Law 107-347, title III, "Federal Information Security Management Act," requires Federal agencies to develop, document, and implement an agencywide information security program and report annually to Office of Management and Budget and Congress on the adequacy and effectiveness of information security policies, procedures, and practices. The Federal Information Security Management Act also requires that each agency develop and maintain an inventory of its major information systems.

The Office of Management and Budget Memorandum M-04-25, "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004, asks agencies about their inventory of major information systems and states that agencies must provide a quarterly update to the Office of Management and Budget on agency information technology security performance measures. The quarterly reports will allow the Office of Management and Budget to assess the security status of information technology for each agency. Office of Management and Budget Circular A-130, "Management of Federal Information Resources," November 28, 2000, establishes policy for information resource management and requires agencies to use a capital planning and investment control process that includes use of information technology portfolios. Finally, Office of Management and Budget Circular A-123 "Management Accountability and Control," June 21, 1995, requires agencies to report annually on management control weaknesses.

Results. To align information technology investments with mission needs and achieve effective portfolio management, DoD officials should establish a definition for an information system and use it to develop and maintain an enterprisewide inventory of information systems; report the lack of an accurate or complete inventory as a material management control weakness; institutionalize the policy on information technology portfolio management stated in the Deputy Secretary of Defense memorandum of March 22, 2004, and issue a Management Initiative Decision on governance and management of information technology portfolios. These steps will allow DoD to better prepare and more accurately respond to Office of Management and Budget and

congressional inquiries, report on expenditures and planned investments, and identify, select, and control investments through the capital planning and investment control process. Finally, the steps will help ensure the integrity of information and reduce the risk of compromise to information technology investments. See the Finding section of the report for the detailed recommendations.

Management Comments. We provided a draft of this report on December 20, 2004. No management comments were received. Therefore, we request that the Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer comment on this final report by February 28, 2005.

Table of Contents

Background

Federal Information Security Management Act. The E-Government Act of 2002, Public Law 107-347, title III, Federal Information Security Management Act (FISMA), requires Federal agencies to develop, document, and implement an agencywide information security program and report annually to the Office of Management and Budget (OMB) and the Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

FISMA requires that each agency develop and maintain an inventory of its major information systems to support information resource management (resource management). Resource management is the way in which an agency manages its information resources, including information and related resources such as personnel, equipment, funds, and information technology (IT), to achieve the agency's mission. FISMA also cites specific resource management actions in existing legislation that include:

- inventorying information resources,
- planning, budgeting, acquiring, and managing IT, and
- monitoring, testing, and evaluating information security controls.

Appendix C provides details on existing resource management legislation cited by FISMA.

OMB FISMA Reporting Instructions. OMB Memorandum M-04-25 "FY 2004 Reporting Instructions for the Federal Information Security Management Act," August 23, 2004, provides agencies with updated instructions for FY 2004 reporting requirements. The instructions include questions that each agency must answer in areas such as performance measures for IT security and inventory of major information systems. The instructions state that OMB expects agencies to have an inventory of major information systems and that agencies must provide OMB with quarterly updates on their IT security performance measures for OMB to use to assess the status of agency IT security. In addition, agencies must report IT security weaknesses in the agency FISMA Report. Significant deficiencies[1] must also be reported as material weaknesses under the Federal Manager's Financial Integrity Act (FMFIA).

OMB Guidance on the Management of Federal Information Resources. OMB Circular A-130, "Management of Federal Information Resources," November 28, 2000, establishes policy for managing information resources. Circular A-130 requires agencies to create an enterprise architecture (EA), use a capital planning and investment control process, and maintain an inventory of major information systems.

[1] A significant deficiency is a weakness in the agency overall information systems security or management control structure that significantly restricts the ability of the agency to carry out its mission or compromises the security of its information systems or other resources, operations, or assets.

EA Defined. The EA is the description and documentation of the current and desired relationships among business and management processes and IT, including a description of the current and target architectures. The agency capital planning and investment control process builds from the current architecture to transition into the target architecture. The EA must be supported with a complete inventory of agency information resources and must include appropriate information security controls.

Capital Planning and Investment Control Process. OMB guidance defines the capital planning and investment control process as an ongoing identification, selection, control, and evaluation of investments for information resources. The process includes establishing security controls, a portfolio of major information systems, and an IT Capital Plan. A portfolio consists of selected IT investments that are managed to prevent redundancy of existing or shared IT capabilities. The IT Capital Plan is the implementation plan for the budget year.

Major Information System. Circular A-130 defines a major information system as one that requires special management attention because of its importance to the agency mission; its high development, operating, or maintenance costs; or its importance in the administration of agency programs, finances, property, or other resources.

Global Information Grid (GIG) Overarching Policy. DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002, provides policy and assigns responsibilities for the GIG architecture and configuration management. The GIG architecture is the globally interconnected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to war fighters, policy makers, and support personnel. The GIG supports all DoD missions with IT assets. Directive 8100.1 requires the establishment and maintenance of an enterprisewide inventory of GIG assets and designates the GIG architecture as the IT architecture required by the Clinger-Cohen Act of 1996. DoD Component heads are required to populate and maintain their portion of the GIG asset inventory and ensure that their architectures are consistent with the GIG architecture.

FMFIA Reporting Guidance. OMB has issued a circular and a memorandum that addresses FMFIA reporting.

OMB Circular A-123. OMB Circular A-123, "Management Accountability and Control," June 21, 1995, was issued under the authority of the FMFIA of 1982. Circular A-123 requires agencies to establish, assess, correct, and report on management controls. In addition, Circular A-123 defines material weaknesses as those management control deficiencies that the agency head determines to be significant enough to report outside the agency. Further, Circular A-123 requires agencies to develop corrective action plans for all material weaknesses, and assess and report progress against those plans periodically. Each agency must report annually material weaknesses in management controls to the President and Congress.

OMB Memorandum. OMB memorandum "FY 2004 Performance and Accountability Reports and Reporting Requirements for the Financial Report of the United States Government," July 22, 2004, provides guidance on preparation and submission of agency Performance and Accountability Reports. The OMB memo indicated that preparation of the Performance and Accountability Report satisfies agency reporting requirements for the FMFIA of 1982. The Performance and Accountability Reports are submitted to OMB and Congress.

DoD Portfolio Management Policy. Deputy Secretary of Defense memorandum, "Information Technology Portfolio Management," March 22, 2004, establishes DoD policy and assigns responsibilities for managing IT investments as portfolios. The Clinger-Cohen Act of 1996 mandates the use of a capital planning and investment control process for IT acquisition, and OMB Circular A-130 mandates that the capital planning and investment control process include portfolio management**.** The Deputy Secretary of Defense assigned the DoD Chief Information Officer with the responsibility to institutionalize the policy within 180 days to become part of the DoD Directive system. DoD Directives transmit information to all DoD Components on how to initiate, govern, or regulate actions.

Management Initiative Decision. A Management Initiative Decision (MID) document is designed to institutionalize management reform decisions. A draft MID pertaining to IT portfolio governance in the spring of 2004 sought to establish a framework for managing IT investments as portfolios. Governance is a single, integrated, hierarchical structure with enterprisewide standards and oversight of IT transformation within DoD. The oversight process describes how and by whom the transformation will be implemented within the DoD.

Objectives

The objective of the audit was to assess the DoD implementation of title III, section 301 "Federal Information Security Management Act of 2002," Public Law107-347. Specifically, we determined whether adequate processes and controls were in place to develop and report on the status of DoD IT systems. See Appendix A for a discussion of the scope and methodology and the review of the management control program. See Appendix B for prior coverage related to the objectives.

Transforming the DoD Management Approach to Information Technology

To align information technology investments with mission needs and achieve effective portfolio management, DoD officials must take the following steps:

- Establish a definition for an information system and use it to develop and maintain an enterprisewide GIG inventory of information systems,
- report the lack of an accurate or complete DoD inventory of GIG systems as a material management control weakness to OMB and Congress,
- institutionalize the policy on IT portfolio management stated in the Deputy Secretary of Defense memorandum, March 22, 2004, which requires IT investments to be managed as portfolios and integrated into the GIG architecture, and
- issue a MID on the governance and management of IT portfolios that allows top-level officials to oversee and approve new or improvements to existing information systems.

These steps will allow DoD to better prepare and more accurately respond to the OMB and congressional inquiries on the status of DoD information systems, to report on DoD expenditure and planned investments, and identify, select, and control investments through the capital planning and investment control process. The steps will also help ensure the integrity of information provided to DoD officials and reduce the risk of compromise to IT investments. They will set into motion the management process for information systems that aligns the DoD EA with the management structure for IT systems that was envisioned by the OMB and the Congress.

Databases for DoD Information Systems

DoD developed and maintains four enterprise-level databases: the Information Technology Management Application (ITMA); the IT Registry; the Business Management Modernization Program (BMMP)[2]; and the DoD Information Technology Portfolio Repository (DITPR). Each database uses different criteria for collecting data about information systems to serve different purposes. See Appendix D for a description of each DoD database. The Government

[2] The DoD BMMP is an effort to transform and modernize DoD business and financial processes and systems. DoD prepared an information system inventory to support the BMMP. We refer to the inventory as the BMMP database. See Appendix D for additional information.

Accountability Office (GAO) and the Inspector General, Department of Defense (IG DoD) reviewed three of the databases which provided insight into their content and structure.

Insight into the Databases. The GAO conducted a review to identify FY 2004 estimated funding for DoD business systems and to determine whether DoD has effective control and accountability over its business system investments. The GAO Report No. 04-615, "DoD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability," May 27, 2004, provided vital information about the content of the ITMA, IT Registry, and BMMP. The report indicated that:

- The ITMA database is used to collect system information to develop the DoD annual IT budget request, but it includes initiatives and programs that are not IT systems.
- The IT Registry database used the terms mission critical and mission essential to identify information systems, but allowed each DoD Component to determine whether a system should be reported as mission critical or mission essential. This self-reporting practice would not necessarily capture the universe of business systems.
- The BMMP database included systems related to DoD business operations; however, DoD did not develop a standard definition of a business system.
- The ITMA, IT Registry, and BMMP system inventory databases contain varying information that overlaps.
- DoD was attempting to reconcile the three databases.

One of the GAO report's recommendations was that the Secretary of Defense direct the Under Secretary of Defense (Comptroller) and the Assistant Secretary of Defense for Networks and Information Integration to develop a standard definition for DoD Components to use in identifying business systems. The DoD response to the GAO report referenced the definition articulated in the Chief Information Officer's July 13, 2004, memo. That memo included a decision tree that used the system definition in DoD Directive 8500.1 "Information Assurance," October 2002, as a foundation for defining a system and then provided additional guidance and examples for clarification. The DoD Directive defined a system as a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. It includes automated information system applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

The Chief Information Officer's July 13, 2004, memo indicated that the definition and decision tree applied to all mission areas and domains and would be used to populate a new database--the DITPR. All DoD systems meeting the definition were to be entered into DITPR by January 2005. On October 20, 2004, the DoD Chief Information Officer issued another memo requiring Components to provide

data on all business systems or families of systems[3] with annual expenditures of $1 million or more to DITPR by January 14, 2005. The October memo required DoD Components to use the definition in DoD Directive 8500.1 as a foundation for defining a system, but provided yet further guidance and clarification than was used in the July 13, 2004 memo. The October memo stated that data on non-business systems or families of systems may be provided, but was not required. As a result, the October 20, 2004, memo reduced the scope of the original DITPR data call for January 2005 from DoD systems in all mission areas and domains to only business systems or families of systems. The July 13, 2004, memo and the October 2004 memo both required that any systems added to DITPR that were not already in the IT Registry must be added to the IT Registry.

The ITMA, IT Registry, and BMMP collected information for different purposes about various systems; thus, they did not use a consistent definition of what constitutes an information system. In addition, the three databases included varying information that overlapped and were not reconciled to each other. The ITMA collected system information for the DoD annual IT budget request, but it also included initiatives and programs that were not IT systems. The IT Registry defined its systems as mission critical and mission essential, but allowed each DoD Component to decide what to report. The BMMP did not use a standard definition for a business system.

The first step in building an inventory is to define an information system. The definition used for DITPR and the decision tree outlined in the July 13, 2004, memo will help DoD define the universe of business systems but not the entire inventory of information systems. To assist DoD IT managers, DoD must decide what to include in its information systems inventory to help frame the definition of an information system. The structure established in the Chief Information Officer's July 2004 and October 2004 memorandums is a start; however, additional work is needed.

Reliability of DoD Databases. DoD included various information from multiple sources, including data calls to DoD Components, in its databases of information systems. The GAO or the IG DoD reviewed three of the databases and identified conditions that affected the usefulness of the data.

ITMA. DoD uses the ITMA database to generate information to prepare budget-related submissions. GAO Report No. 04-615 reported that the ITMA database also includes initiatives and programs that are not IT systems.

IT Registry. The IT Registry includes DoD mission-critical and mission-essential systems. DoD Components are responsible for populating the IT Registry, updating and maintaining the information, and certifying the accuracy and completeness of the data. According to December 2003 IT Registry guidance, Components are to add all nonmission-critical and nonmission-essential systems to the IT Registry by September 30, 2006. The IG DoD Report No. D-2003-117, "Systems Inventory to Support the Business Enterprise Architecture," July 10, 2003, stated that the DoD IT Registry would not necessarily capture the

[3] A family of systems is a set of independent systems that can be arranged or interconnected in various ways to provide different capabilities.

universe of business systems because IT Registry guidance did not require all business management systems to be reported, and because system definitions in the registry guidance are subject to interpretation. In addition, IG DoD Report No. D-2003-008, "Implementation of the Government Information Security Reform by the Defense Finance and Accounting Service for the Defense Integrated Financial System," October 7, 2002, stated that DoD did not require the IT Registry software to include data integrity controls that would ensure the accuracy, completeness, and validity of information in the database.

BMMP. As of April 2003, DoD used multiple sources, including data calls, to identify an inventory of 2,274 business systems. In July 2004, the Acting Under Secretary of Defense (Comptroller) testified that DoD was establishing a progressively more comprehensive business system inventory and had identified more than 4,000 systems, with more systems likely to be identified in the future. In GAO Report No. 04-615, GAO determined that DoD does not have an accurate inventory of its business systems because it lacks a central repository, a systematic way to identify its business systems, and a standard definition of what constitutes a business system. The report stated that the initial repository of 2,274 DoD business systems is neither complete nor informative enough for use in decision making.

Although each database serves a different purpose, each experienced problems in the ability to use the data to develop a complete and accurate inventory of DoD information systems resulting from problems with the content, accuracy, or completeness of the data. FISMA reporting instructions and guidance require the security controls of information systems to be monitored, tested, and evaluated. OMB requires agencies to provide quarterly updates of their IT security performance measures that will permit OMB to assess agency IT security status. DoD information systems must be protected to ensure an appropriate level of confidentiality, integrity, availability, and accountability and to ensure that DoD operations and missions are not disrupted. Until a complete and accurate inventory is identified and verified, there is little assurance that DoD knows the status of its systems.

DoD Instruction 5200.40, "DoD Information Technology Security Certification and Accreditation Process (DITSCAP)," December 30, 1997, creates the DoD process for security certification and accreditation of information systems. The objective of the process is to establish a standard approach to protect and secure the entities that comprise the Defense Information Infrastructure. Standardizing the certification and accreditation process minimizes the risks associated with nonstandard security implementations across shared infrastructure and end systems. To ensure that information systems are protected and subjected to the certification and accreditation process, DoD must be aware of the existence of its information systems. Otherwise, there is no assurance that the DoD enterprise itself is adequately protected.

Material Management Control Weakness

FMFIA Reporting for FY 2003. OMB Circular A-123, "Management Accountability and Control," June 21, 1995, was issued under the authority of the FMFIA of 1982 and requires agencies to report annually on management control weaknesses. For FY 2003, DoD reported nine systemic weaknesses in the FMFIA section of its Performance and Accountability Report. The weaknesses identified that the DoD financial and business management systems and processes were not fully integrated and did not provide reliable, timely, and accurate information. In addition, DoD officials reported that they need to better manage IT and need assurance that IT is adequately protected. DoD also reported a weakness in the IT Capital Investment Process in that the process does not confirm that the best investments are selected, deliver expected benefits, or perform as expected.

Inventory of Major Information Systems. In answering OMB questions on the information system inventory**,** DoD stated that it uses the DoD IT Registry to maintain an inventory of DoD major information systems. However, past reviews found that the IT Registry would not necessarily include all major systems and was not integrated with other information system databases. As a result, DoD cannot be assured that it has a complete inventory of major information systems. This is a material management control weakness in DoD resource management that DoD did not report as a component of the systemic weakness in IT management and assurance under the FMFIA.

If DoD does not have a complete inventory of major information systems, planning improvement or system replacement is difficult, answers to questions from OMB or Congress on major information systems may not be accurate, and information assurance is at risk because there is little assurance that all systems are adequately protected. In addition, DoD cannot build an EA and initiate the capital planning and investment control process. DoD must report the lack of an inventory of major information systems as a component of the systemic weakness in IT management and assurance in future DoD FMFIA reporting until DoD can develop and manage a GIG information system inventory.

Portfolio Management Process-Recent Events

DoD Portfolio Management Policy. The Deputy Secretary of Defense memorandum, "Information Technology Portfolio Management," March 22, 2004, established DoD policy and assigned responsibilities for managing IT investments as portfolios. Portfolio management is defined as the management of selected groupings of IT investments using integrated architectures, measures of performance, risk management techniques, transition plans, and portfolio management strategies. The Clinger-Cohen Act of 1996 mandated the use of a capital planning and investment control process for IT acquisition, and OMB Circular A-130 mandated that the capital planning and investment control process include portfolio management. The Deputy Secretary's memo stated that the decisions on which investments to make, modify or terminate should be based on

the GIG integrated architecture, mission area goals, architecture, risk, potential return, and outcome goals and performance. The memo also stated that the portfolio management process should consist of the following core activities.

- analysis that links mission area goals to DoD enterprise vision, goals, and objectives and how those will be achieved and measured; identifies gaps and opportunities; identifies risks and how they will be mitigated; provides a continuous process improvement; and determines strategic direction for mission area activities and processes,

- selection that identifies the best mix of IT investments to achieve outcome goals and plans and transition to "to be" architectures,

- control which ensures that a portfolio and individual projects in the portfolio are acquired in accordance with cost, schedule, performance, and risk baselines and are within the scope of the currently approved version of the GIG architecture, and

- evaluation that routinely and systematically assesses and measures actual contributions of the portfolio as well as supports adjustments to the mix of portfolio projects as necessary.

The guidance also sets policy that integrated architectures require mission area domains and DoD Component perspectives to better understand the organization and the capability gaps between the current and future environments. A mission area is a defined area of responsibility whose functions and processes contribute to accomplishment of the mission. In March 2004, the Deputy DoD Chief Information Officer testified that DoD uses the following three mission areas for portfolio management: war fighter, business, and enterprise information environment. Domains within mission areas are a common collection of related, dependent information capabilities. An integrated architecture consists of multiple views that facilitate integration and promote interoperability and compatibility among related architectures.

The Deputy Secretary's March 22, 2004, memo states that integrated architectures must be developed to assess the process improvement opportunities within and across all levels, determine interoperability and capacity requirements, promote standards, identify and implement information assurance requirements, formulate and target investments to improve data and information management, and identify the required capabilities of the technical infrastructure.

To implement his policy, the Deputy Secretary assigned the following responsibilities to the DoD Chief Information Officer:

- Ensure that business and war fighting integrated architectures comply with the GIG.

- Establish a process for maximizing value and assessing and managing IT investment risk.

- Coordinate with the Principal Staff Assistants and the Chairman of the Joint Chiefs of Staff to provide a core set of uniformly applied criteria for portfolio management and selection.

- Institutionalize the policy within 180 days to become part of the DoD Directive system. DoD Directives provide information to DoD Components on initiating, governing, or regulating actions.

The policy also assigns responsibility to the DoD Principal Staff Assistants to establish business domains in coordination with the DoD Chief Information Officer and a repeatable portfolio management process that includes a governance structure.

As of December 2004, the policy has not been institutionalized. The Deputy Secretary's memo began a process within DoD to rethink how IT investments should be acquired and managed more consistently with legislative requirements, to include the Paperwork Reduction Act of 1995, and subsequent OMB guidance. The Deputy Secretary's memo stated that IT should be managed as portfolios, and the portfolio management process should be established and include certain core activities. The memorandum initiated a significant shift within the DoD on how it views and manages IT systems. DoD must now institutionalize the March 2004 policy in a DoD Directive that mandates change in the way DoD views and manages IT investments.

Redefining the Management of IT Systems

MID. A MID document is designed to institutionalize management reform decisions. A draft MID pertaining to IT portfolio governance in the spring of 2004 indicated that IT investments were defined and managed using an individual, platform, or system approach rather than a mission approach. These approaches allowed duplicative investments in systems to deliver the same or similar capabilities.

The draft MID instituted the concept of portfolio management and changed the management approach to IT. The MID established a governing authority to create and enforce policies to integrate the three DoD mission areas. The MID provides a framework that will allow mission area officials to manage IT investments as portfolios, implement DoD guidance, and finance activities within their areas. The mission area senior officials will define domains within their mission area, assign IT programs to a domain, and establish a governance process. The domain owners manage portfolios of information capabilities and services. The domain owners justify new capabilities; identify requirements for new programs; review, assess, and approve the DoD Components' funding for IT programs; review programs for performance against capability requirements and schedules; maintain an inventory of systems in the domain; and develop and maintain a GIG-compliant domain architecture. A key point is that the MID requires the Principal Staff Assistants for the mission areas to finance activities of the mission areas and the DoD Chief Information Officer to issue DoD guidance for portfolio management.

DoD needs to enact a MID or comparable DoD Directive to implement congressional intent with regard to IT management, as expressed in the National Defense Authorization Act of FY 2005, to provide a consistent portfolio management process for all DoD mission areas, including domain review and approval of Component funding for all IT investments. The new guidance would significantly reduce the risk of Component stove-piping of IT systems and would fund and field only those IT investments needed to fulfill the DoD mission that is integrated into the overarching architecture.

Conclusion

An asset inventory is the foundation for all portfolio management activities. Without a complete inventory of information systems, DoD cannot respond accurately to inquiries from Congress and OMB on the status of information systems, efficiently plan for future enhancements or replacement systems, prevent duplication of systems, report accurately on DoD expenditure for IT, and implement a system management process that is consistent with the EA. DoD assembled different databases for different purposes and used different definitions for an information system. The DITPR database is a positive step; however, additional efforts are needed. Before an inventory can be developed, DoD must develop a definition for an information system and use it consistently. Next, DoD must select a platform to host the inventory; establish procedures to address control of and input to the database; and establish a mechanism to oversee the effort, verify the input, and ensure that all information systems are entered.

The requirement for an inventory has existed for a long time; however, DoD has not established a complete inventory of its information systems or consistently defined an information system. Until these tasks are accomplished, DoD must report its lack of a major information system inventory in its annual reporting to OMB and Congress. Finally, restructuring IT management within DoD will begin a management process for information systems that aligns the DoD EA with the management structure for information systems that OMB and Congress envisioned.

The Deputy Secretary's memo began a process within DoD that rethought how IT investments should be acquired and managed more consistently with legislative requirements such as the Paperwork Reduction Act of 1995 and subsequent OMB requirements. DoD must institutionalize the policy in the March 22, 2004, memo in a DoD Directive to mandate change in the way DoD views and manages IT investments. Directions in the draft MID and congressional intent pertaining to IT management in the National Defense Authorization Act for FY 2005 must also be implemented as a further step in redefining how DoD manages and funds its IT investments as portfolios.

Recommendations

1. We recommend that the Assistant Secretary of Defense for Networks and Information Integration:

a. Develop and staff a DoD Directive to:

(1) Establish a definition for an information system that applies to all mission areas;

(2) Require use of the definition to develop and maintain an enterprisewide inventory of information systems; and

(3) Institutionalize the policy contained in the Deputy Secretary of Defense memorandum of March 22, 2004, on information technology portfolio management.

b. Document in the DoD Federal Managers Financial Integrity Act and Federal Information Security Management Act Reports that DoD does not have an accurate or complete inventory of major information systems.

2. We recommend that the Under Secretary of Defense (Comptroller)/Chief Financial Officer forward the draft Management Initiative Decision on governance and management of information technology portfolios to the Deputy Secretary of Defense for decision.

Management Comments Required

The Under Secretary of Defense (Comptroller)/Chief Financial Officer and the Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer did not comment on a draft of this report. We request that the Under Secretary and the Assistant Secretary provide comments on the final report.

Appendix A. Scope and Methodology

We reviewed the Clinger-Cohen Act of 1996 and other legislation on resource management. We also reviewed the FISMA sections on information system security and inventory requirements, OMB guidance on resource management, the FMFIA, DoD documentation describing four DoD information system databases, and GAO and IG DoD audit reports on databases. Further, we reviewed documentation and guidance on IT investment portfolio management and a proposal to restructure the DoD management of IT investments.

We used pertinent guidance to assess DoD resource management practices, specifically the development and maintenance of an inventory of major information systems. We also considered proposals to modify the overall management of DoD IT investments and assessed DoD compliance on FMFIA reporting. We reviewed data from May 1995 through November 2004.

We performed this audit from April through December 2004 in accordance with generally accepted government auditing standards.

Use of Computer-Processed Data. We did not use computer-processed data to arrive at the conclusions in this audit report.

Use of Technical Assistance. We did not use technical assistance to perform this audit.

Government Accountability Office High-Risk Area. The GAO has identified several high-risk areas throughout the Federal Government. This report covers the Protecting Information Systems Supporting the Federal Government and the Nation's Critical Infrastructures area. In addition, GAO also identified several high-risk areas in DoD. This report covers the Defense Systems Modernization high-risk area.

Management Control Program Review

DoD Directive 5010.38, "Management Control (MC) Program," August 26, 1996, and DoD Instruction 5010.40, "Management Control (MC) Program Procedures," August 28, 1996, require DoD organizations to implement a comprehensive system of management controls that provides reasonable assurance that programs are operating as intended and to evaluate the adequacy of the controls.

Scope of the Review of the Management Control Program. We did not announce a review of the management control program as an audit objective because DoD recognized the management of IT and information assurance as a systemic weakness in the FY 2003 FMFIA report. Accordingly, we did not review management's self-evaluation. However, we reviewed DoD compliance with the FISMA of 2002 requirement to maintain an agency inventory of major information systems to support resource management. We also reviewed the DoD FY 2003 FMFIA report.

Adequacy of Management Controls. We identified a material management control weakness for DoD as defined by DoD Instruction 5010.40. DoD management controls for IT management and information assurance were not adequate to ensure that DoD developed and maintained an enterprisewide inventory of major information systems in accordance with the FISMA of 2002. Recommendation 1., if implemented, will improve DoD compliance with the FISMA inventory requirement. A copy of the report will be provided to the senior official responsible for management controls in the Office of the Assistant Secretary of Defense for Networks and Information Integration.

Appendix B. Prior Coverage

During the last five years, GAO and the IG DoD have issued 14 reports related to DoD management of IT resources. Unrestricted GAO reports can be accessed over the internet at http://www.gao.gov. Unrestricted IG DoD reports can be accessed at http://www.dodig.osd.mil/audit/reports.

GAO

GAO Report No. GAO-04-907T, "Department of Defense: Long-standing Problems Continue to Impede Financial and Business Management Transformation," July 7, 2004

GAO Report No. GAO-04-376, "Information Security: Agencies Need to Implement Consistent Processes In Authorizing Systems for Operation," June 28, 2004

GAO Report No. GAO-04-615, "DoD Business Systems Modernization: Billions Continue to Be Invested with Inadequate Management Oversight and Accountability," May 27, 2004

GAO Report No. GAO-04-731R, "DoD Business Systems Modernization: Limited Progress in Development of Business Enterprise Architecture and Oversight of Information Technology Investments," May 17, 2004

GAO Report No. GAO-04-551T, "Department of Defense: Further Actions Needed to Establish and Implement a Framework for Successful Financial and Business Management Transformation," March 23, 2004

GAO Report No. GAO-04-115, "Information Technology: Improvements Needed in the Reliability of Defense Budget Submissions," December 19, 2003

IG DoD

IG DoD Report No. D-2004-081, "Reporting of DoD Capital Investments for Information Technology," May 7, 2004

IG DoD Report No. D-2003-117, "Systems Inventory to Support the Business Enterprise Architecture," July 10, 2003

IG DoD Report No. D-2003-022, "FY 2002 Independent Assessment of the DoD Subset of Information Technology Systems for Government Information Security Reform Reported for FY 2001," November 14, 2002

IG DoD Report No. D-2003-008, "Implementation of the Government Information Security Reform by the Defense Finance and Accounting Service for the Defense Integrated Financial System," October 7, 2002

IG DoD Report No. D-2001-182, "Information Assurance Challenges-A Summary of Results Reported April 1, 2000 Through August 22, 2001," September 19, 2001

IG DoD Report No. D-2001-175, "Application of Year 2000 Lessons Learned," August 22, 2001

IG DoD Report No. D-2001-096, "Management of Information Technology Equipment, Office of the Secretary of Defense," April 9, 2001

IG DoD Report No. D-2000-162, "Summary of Audits of Acquisition of Information Technology," July 13, 2000

Appendix C. Legislation for Management of Federal Information Resources

FISMA. Public Law 107-347, FISMA, requires agencies to develop and maintain an inventory of major information systems operated by or under the control of the agency and to use the inventory to support resource management activities. FISMA requires the inventory to support the preparation and maintenance of information resources under section 3506(b)(4), title 44, United States Code. The Paperwork Reduction Act of 1995 (Public Law 104-13) amended chapter 35, title 44, United States Code to include section 3506(b)(4) requiring an inventory of agency information resources.

FISMA also requires the major system inventory to support IT planning, budgeting, acquisition, and management under section 3506(h), title 44, United States Code, subtitle III of title 40, United States Code, and related laws and guidance.

- The Paperwork Reduction Act of 1995 (Public Law 104-13) amended chapter 35, title 44, United States Code to include section 3506(h) requiring agencies to maximize the value and assess and manage risks of major information system initiatives by developing a process to select, control, and evaluate results of such initiatives.

- The Clinger-Cohen Act of 1996 (Public Law 106-104), section 5122 supplemented section 3506(h), title 44, United States Code by requiring that agencies use a capital planning and investment control process to provide for selection, management, and evaluation of IT investments. Public Law 107-217 recodified the Clinger-Cohen requirement as section 11312 under subtitle III, title 40, United States Code.

FISMA requires the major system inventory to support monitoring, testing, and evaluation of information security controls under subchapter II, title 44, United States Code. The National Defense Authorization Act for FY 2001, subtitle G, "Government Information Security Reform," amended chapter 35, title 44, United States Code by inserting subchapter II, which requires agencies to establish, test, and evaluate information security controls. The Government Information Security Reform requirements have been replaced by the requirements of FISMA.

FISMA requires the major system inventory to support preparation of the index of major information systems required under section 552(g), title 5, United States Code. The Electronic Freedom of Information Act Amendments of 1996 amended section 552 of title 5 United States Code to add subsection (g) that required an index of agency major information systems.

Appendix D. DoD Information Systems' Databases

DoD developed four databases: the ITMA, the IT Registry, the BMMP, and the DITPR. Each database uses different criteria for collecting data about information systems and collects the data to serve different purposes.

ITMA. According to the DoD Financial Management Regulation, the ITMA is a database application to plan, coordinate, edit, publish, and disseminate IT budget information for Congress and OMB. DoD Components are required to register their IT resources as initiatives in ITMA. Initiatives can be systems, families of systems, programs, projects, organizations, or activities.

IT Registry. The FY 2001 National Defense Authorization Act requires DoD to maintain an inventory of mission-critical and mission-essential information systems. According to DoD IT Registry guidance, the DoD IT Registry is the enterprisewide systems inventory used to fulfill the Act's requirements and to prepare reports in response to FISMA, OMB and Congress.

BMMP. The DoD BMMP is an effort to transform and modernize DoD business and financial processes and systems. The program includes development of a business EA as a blueprint for DoD business transformation. Business processes include financial, logistical, personnel, and procurement processes. The FY 2003 National Defense Authorization Act (Public Law 107-314) required DoD to develop an inventory of DoD systems to support the business EA that was based on a system definition to be developed by the Under Secretary of Defense (Comptroller). DoD responded by preparing an information system inventory to support the BMMP.

DITPR. In July 2004, DoD issued guidance on a new database, entitled the DITPR, which will support DoD portfolio management by collecting data on DoD information systems in all mission areas and domains. The guidance requires submission of information on selected business systems, with data on remaining DoD information systems to be collected later. In October 2004, DoD issued additional guidance requiring data to be submitted on remaining business systems or families of business systems.

Appendix E. Report Distribution

Office of the Secretary of Defense

Under Secretary of Defense for Acquisition, Technology, and Logistics
Under Secretary of Defense (Comptroller)/Chief Financial Officer
    Deputy Chief Financial Officer
    Deputy Comptroller (Program/Budget)
    Director, Business Management Modernization Program
Under Secretary of Defense for Personnel and Readiness
Under Secretary of Defense for Intelligence
Assistant Secretary of Defense for Networks and Information Integration/Chief Information Officer
Director, Program Analysis and Evaluation

Joint Staff

Director, Joint Staff

Department of the Army

Auditor General, Department of the Army

Department of the Navy

Naval Inspector General

Department of the Air Force

Assistant Secretary of the Air Force (Financial Management and Comptroller)

Other Defense Organization

Director, Defense Information Systems Agency

Non-Defense Federal Organization

Office of Management and Budget

Congressional Committees and Subcommittees, Chairman and Ranking Minority Member

Senate Committee on Appropriations
Senate Subcommittee on Defense, Committee on Appropriations
Senate Committee on Armed Services
Senate Committee on Governmental Affairs
House Committee on Appropriations
House Subcommittee on Defense, Committee on Appropriations
House Committee on Armed Services
House Committee on Government Reform
House Subcommittee on Government Efficiency and Financial Management, Committee on Government Reform
House Subcommittee on National Security, Emerging Threats, and International Relations, Committee on Government Reform
House Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform

Team Members

The Office of the Deputy Inspector General for Auditing of the Department of Defense, Acquisition and Technology Management prepared this report. Personnel of the Office of the Inspector General of the Department of Defense who contributed to the report are listed below.

Thomas Bartoszek
Barry Gay
John Huddleston
James Mitchell
Alejandra Rodriguez
Vicky Sain
Christopher Scrabis
Kathryn Truex